

公告本

申請日期	88 年 1 月 20 日
案 號	88100822
類 別	H04L 9/32
Int. Cl.	

A4
C4

421955

以上各欄由本局填註)

發明專利說明書

一、發明 名稱	中 文	傳送資訊於用戶識別模組及無線通訊行動終端間之方法；及相關用戶識別模組及行動終端
	英 文	A method of transferring information between a subscriber identification module and a radiocommunication mobile terminal, and a corresponding subscriber identification module and mobile terminal
二、發明 創作人	姓 名	(1) 佛瑞德瑞克·凡斯尼爾 Vasnier, Frederic (2) 安妮·李隆吉爾伯特 Lelong-Gilbert, Anne Gaelle (3) 巴斯卡·修比 Hubbe, Pascal
	國 籍	(1) 法國 (2) 法國 (3) 法國
	住、居所	(1) 法國可倫畢斯佛斯波思路一〇三一一〇五號 103-105 rue des Voies du Bois, 92700 Colombes, France (2) 法國威洛弗雷約瑟夫伯特蘭路一〇三號 103 rue Joseph Bertrand, 78220 Viroflay, France (3) 法國巴黎布雷辛路七號 7, rue Brezin, 75014 Paris, France
	代 表 人 姓 名	(1) 艾可特公司 ALCATEL
三、申請人	姓 名 (名稱)	(1) 艾可特公司 ALCATEL
	國 籍	(1) 法國
	住、居所 (事務所)	(1) 法國巴黎玻璃堤路五十四號 54, rue La Boetie, 75008 Paris, France
	代 表 人 姓 名	(1) 凡微麗·費瑞 Feray, Valerie

裝

訂

線

申請日期	88 年 1 月 20 日
案 號	88100822
類 別	

A4
C4

(以上各欄由本局填註)

發 明 專 利 說 明 書
新 型

一、發明 新型名稱	中 文	
	英 文	
二、發明 創作人	姓 名	(4) 克里斯多夫·巧魁特 Choquet, Christophe
	國 籍	(4) 法國
	住、居所	(4) 法國巴黎維特杜魯易路三號 3, rue Victor Duruy, 75015 Paris, France
三、申請人	姓 名 (名稱)	
	國 籍	
	住、居所 (事務所)	
	代 表 人 姓 名	

裝

訂

線

421 955

(由本局填寫)

承辦人代碼：
大 類：
I P C 分類：

A6
B6

本案已向：

國(地區) 申請專利, 申請日期: 案號: , ☐有 ☐無主張優先權
法國 1998 年 1 月 26 日 98 00771 ☒有主張優先權

有關微生物已寄存於: , 寄存日期: , 寄存號碼:

(請先閱讀背面之注意事項再填寫本頁各欄)

裝

訂

線

五、發明說明(1)

[發明領域]

本發明之領域為通訊系統，更明白地說但並不排除，例如 G S M (行動通訊之泛用系統) 及 D C S 1 8 0 0 系統 (數位蜂巢式系統)。

[發明背景]

一般來說，於上述系統中，使用者經由一行動台通訊，該行動台包含一行動終端，其配合一用戶識別模組 (S I M)，該模組通常被稱為一 S I M 卡。

推薦書 G S M 1 1 . 1 1 指定有關於由無線通訊網路所提供之服務應被儲存於 S I M 卡之記憶體區域上，以類似於用戶識別資料之方法。

歐洲電信標準 (E T S) 定義於用戶識別模組及行動終端間之界面。

依據推薦書 G S M 1 1 . 1 1 及 1 1 . 1 4，一組有關於 S I M 卡之使用之命令，其被稱為 S I M 應用工具組，於以下被稱為 S I M 命令組。

S I M 命令組組合一組應用及相關程序，其係可以於行動終端及相關 S I M 卡間之通訊交談時被使用。

S I M 卡大致為一智慧卡，用以個人化行動台。當於具有丟掉或被偷之高度危險而最後造成盜打之手持行動終端時，有必要以個人化行動台。

提供給使用者之用以限制盜打危除之解答是使用一可移除 S I M 卡，該使用者可以當要與終端分離時，自行動

五、發明說明(2)

終端將其拆下。沒有了S I M卡，行動終端只可提供有限類型之呼叫，特別是緊急呼叫之服務。

然而，這方法對該問題並不是完整之解答。對於未授權之行動終端持有人仍有可能模擬正常相關於該終端之S I M卡，以可能於截收於行動終端及S I M卡間之常態訊息互換之後，作為行動終端之盜打目的。

這類型盜打已經成為一嚴重威脅，因為所謂“預付”卡之引入。於包含有此類型卡之站之（欺騙）識別後，使用該台就沒有限制，因為該呼叫時間係被計價至包含於該卡上之預付帳上。這情形是類似於由預付卡計價預付帳之情形（騙徒然後負責該帳號）。

〔發明目的及概要〕

本發明目的為提供上述問題之解答，使得任何類型之欺騙很困難，而變得不可達成。

有關此方面，因此，本發明包含一種用以傳送資訊於一用戶識別模組及構成無線通訊系統之一台之一行動終端間之方法。依據本發明至少部份被傳送於模組及終端間之資訊係藉由加密而加以保護，該加密係藉由使用於該模組及終端中之一鑰。該鑰係至少部份藉由該系統之週期變化資料所定義。

依據本發明，該週期變化資料是為專屬於該無線通訊系統之時鐘之函數。

同時，該鑰是較佳地部份地被專屬於行動台之其他資

五、發明說明(3)

料所定義。

定義該鑰之資料係較佳組合於該模組及該終端中，於每次被加密所保護之資料之傳送之時。

本發明同時包含一行動終端及一S I M卡，分別適用以應用該加密資訊傳送方法。

[圖式之簡要說明]

本發明之其他特性及優點可以由以之本發明之實施例之說明參考附圖而作非限定例示，附圖中：

第1圖為依據本發明之用戶識別模組之實施例之簡化方塊圖；

第2圖為依據本發明之行動終端之實施例之簡化方塊圖，並被設計以配合第1圖之用戶識別模組；

第3圖為本發明之資訊傳送方法之簡化流程圖；

第4圖示出由一行動終端傳送至一用戶識別模組之訊息，用以配合第3圖之方法；及

第5圖示出用以取得於第1圖之用戶識別模組中之加密鑰之機構。

主要元件對照表

10	S I M卡
12	連接接觸區域
13	半導體晶片
14	資料處理機構

五、發明說明(4)

1 5	雙向匯流排
1 6	傳送單元
1 7	記憶體
1 8	加密單元
1 7 1	永久記憶體
1 7 2	草稿記憶體
1 9	記憶體區域
2 0	行動終端
2 1	資料處理機構
2 3	記憶體
2 4 - 2 6	界面裝置
2 8	螢幕
2 9	按鍵墊
2 1 0	麥克風／喇叭組合
2 1 1	接觸元件
2 1 2	加密
2 7	傳送裝置
2 3 1	位置

〔詳細說明〕

以下說明有關於本發明之應用至 G S M 無線通訊系統之特定例子。熟習於本技藝者可以知道於此之原理並不只可適用於所述之 D C S 1 8 0 0 系統，同時也可以用於其他類型之無線通訊系統。

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明(5)

第1圖為一SIM卡10之實施例之一般方塊圖，其包含特別一支持件11，其承載連接接點區域12及一半導體晶片13。晶片13包含資料處理機構14（典型地一微處理機），連接至一雙向匯流排15，經由傳送單元16連接匯流排15至接點區域12，及連接至記憶體17。一加密單元18係連接至該傳送單元16及記憶體17具有一專屬於加密資訊之區域19。

記憶體17傳統包含永久記憶體171，用以儲存電話用戶資料，而使得可以用併入有SIM卡10之行動台，並具有為微處理機14所執行之程式。資料可以被儲存於其中，藉由一無線通訊網路之操作者或者一銷售代表，並一般為永久性質。然而，一些資料可以藉由微處理機14之特殊動作而修改，並因此為一半永久性質。記憶體17同時包含一草稿記憶體172，被微處理機所使用以儲存來自行動終端之資料，SIM卡10係被插入於行動終端中，以及，一些由微處理機14所執行處理而產生之資料必須被傳送至行動終端。記憶體區域19係較佳被分離於永久記憶體171及草稿記憶體172之間，如同以下參考第5圖所描述。

開始為不作動之SIM卡之操作之一般模式包含由上述SIM命令組之應用中之行動終端所啓始之交談，並造成資料被傳送經由接點區域12至傳送單元16至微處理機14。反應及配合記憶體17，微處理機14執行由永久記憶體171所取出之程式，使得其儲存由行動終端所

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

線

五、發明說明(6)

供給之資料於草稿記憶體 1 7 2，以處理此資料，並由永久記憶體 1 7 1 取出其他資料，以準備被儲存於草稿記憶體 1 7 2 中之處理結果。於此文中，微處理機 1 4 同時使得準備於記憶體 1 7 2 中之所得資料被經由傳送單元 1 6 傳送至行動終端。該交談完成，及當資料傳送（可能為多資料傳送）完成時，S I M 卡再次變成不作動。

依據本發明，該卡藉由加入加密單元 1 8 及加密資訊記憶體區 1 9，使得上述之資料傳送係被加密所保護。加密類型於本身係為已知的於此並不需要說明。其需要於加密單元 1 8 中組合與予以傳送之資料之鑰（一祕密加密資料序列），以提供一不為其他任何持有鑰以外人所能理解之序列信號，以進行交談解密操作，以重建原始資訊。該鑰係產生於加密單元 1 8 中，藉由使用由微處理機 1 4 所準備並經由匯流排 1 5 傳送之鑰資訊。這是藉由以下參考第 3 圖之本發明之資訊傳送方法之說明加以討論。

第 2 圖為一行動終端 2 0 之實施例之一般方塊圖，其包含經由一雙向匯流排 2 2 相關於一記憶體 2 3，及控制終端之其他機構之組合之資料處理機構 2 1（典型為一微處理機）。

微處理機 2 1 控制各種界面裝置 2 4 至 2 6，分別相具有一螢幕 2 8，一按鍵墊 2 9 及麥克風／喇叭組合 2 1 0。特別是，其控制相關於接點元件 2 1 1 之傳送裝置 2 7，該元件 2 1 1 與被插入於終端中之 S I M 卡之接點區域接觸。另外，依據本發明，一加密裝置 2 1 2 係連

五、發明說明(7)

接至傳送單元 2 7，以及，記憶體 2 3 包含被指定給加密資訊之位置 2 3 1。

行動終端 2 0 之操作將不再於此說明，因為這將超出本發明之範圍。只要說行動終端使用儲存於 S I M 卡上之資訊就行了。行動終端之微處理機 2 1 啓始一交談，應用上述 S I M 命令組，並造成資料以兩方向傳送經由傳送裝置 2 7 及接點元件 2 1 1，於相關於第 1 圖之說明中所定義者。

依據本發明及已經說明者，行動終端係藉由加入加密裝置 2 1 2 及加密資訊記憶體位置 2 3 1，而適用以藉由加密保護資料傳送。

第 3 圖示出本發明之一實施例，其中有一方法以傳送資訊於例如第 1 圖之 S I M 卡之用戶識別模組及例如第 2 圖之行動無線通訊終端間。

例如，假若使用者剛才按下按鍵墊 2 9 上之按鍵，以打電話出去。最後按下的是一確認鍵，並使得終端改變 S I M 卡，以檢查是否呼叫被授權否，及當於預付卡時檢查是否有足夠額度用於該呼叫。

於第 1 步驟 3 1 中，行動終端使用 S I M 命令組，用於呼叫控制交談之目的。該交談係由幾部份作成。第一部份，使用者輸入，開始於一呼叫步驟 3 1，其包含 S I M 卡被啓始及行動終端送出一如第 4 圖所示之訊息 4 1 給 S I M 卡（或更明確地說給卡上之微處理機）。該訊息包含資料 S T，其指明其為 S I M 命令之一部份，資料 T S

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

線

五、發明說明(8)

指明交談類型(於此為使用者輸入)，及指示S指明其為交談之第一訊息，及最後時間資料。時間資料是隨著時間改變之資訊，並係專屬於該無線通訊系統，使得其不必提供機構，以用於創造該資料，並且只要將其於行動終端由一裝置中讀出，該裝置係已被終端所包含用於其他目的者；該資訊係有利地為被稱為“GSM時鐘”之時間資訊，其包含如於GSM系統所知之元件T1，T2，T3，並被GSM標準之推薦書05.02及05.10所定義。當然，步驟31同時包含此訊息之接收於SIM卡上。這步驟係不使用加密下完成，即行動終端之加密單元212及SIM卡之加密單元18不作動，並不涉及該傳送。

上述訊息之傳送造成一計算鍵步驟32，以示於第5圖之方式計算一加密鑰。第5圖更特別有關於SIM卡上執行上述計算，但相同計算同時被執行於行動終端中(見以下)。永久記憶體17之區域171.1含有一母鑰CM。其係專屬於製造者或操作者並被以相同於其他電話用戶資料之時間加以儲存。記憶體17之另一區域171.2包含一IMEI(國際行動設備身份)，其是一數字專屬於該行動終端並被儲存於該卡上，如前所述當不再租用時被取出。最後，時間資料係暫時地被儲存於步驟31中，於草稿記憶體172之區域172.1中。上述三個元件係被一組合裝置51所組合，以產生一鑰產生指示CS於52。組合裝置51可以硬體接線於加密單元18中，微處理將三元件送給它，或其可以是由微處理機

五、發明說明(9)

14 所執行之程式，其然後直接供給 CS 指示給加密單元 18。

同時，以不必詳述之方式，相同之處理係執行於行動終端中，於記憶體 23 中之統稱為 231 之位置係以相同方式包含上述之三元件，及用以依據第 5 圖組合它們之機構係被提供，以取得一鑰產生器指示，其係最終可用於加密裝置 212 之中。

然後，一認可步驟 33 基本上包含於 SIM 卡中被傳送至行動終端之認可信號，該信號包含一指令以執行加密傳送。這同時作動了有關於被以兩方式傳送資料之加密單元 18 及加密裝置 212，該兩方式係經由在資料傳送卡之終端 / SIM 卡界面，於傳送單元 16 或傳送裝置 27 及源或目的單元間，即在 SIM 卡上之處理機 14 或記憶體 172，於行動終端中之微處理機 21 或記憶體 23 之間。

於傳送 1 上之此點，．．．，以加密形式傳送資料，傳送 N 步驟 34，．．．35。涉及 SIM 卡之傳送，即使於接點區域 12 或接點元件 211 被截收，也不會被濫用。也不會被竄改。因而，完成了本發明之目的。

相同於 SIM 卡及行動終端中之鑰產生器指示係被用於鑰產生裝置加密單元 18 及加密裝置 22 中，並產生兩相同鑰，一用以於發送端加密，而另一個用於接收端解密。該鑰產生裝置係例如一反應型移位暫存器。

於前述有關於使用者輸入資料傳送之步驟 31 至 35

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明(10)

後，第3圖示出有關於一呼叫設立傳送，其係為包含於SIM命令組之傳送之一，其中，一呼叫已授權步驟36包含一訊息之加密傳送，該訊息指示為步驟31所定義之呼叫被授權。結果，該呼叫係被行動終端依據GSM系統加以傳送。同時，一顯示本文傳送之顯示步驟37命令於行動終端螢幕上顯示一相當於處理中之呼叫操作之文字。於此交談結束時，於結束步驟38中，加密單元18及加密裝置212係被關閉。先前使用鑰並不可用。該交談被關閉。另一交談必須發生於剛才所述之模式中。

明顯地，前述說明可以允許很多不脫離本發明之申請專利範圍中所定義之變化。特別是，鑰之合成可以不同，於其包含與系統有關之改變資訊時。因此，IMEI可以以其他專屬於該預約並為SIM卡及行動端所使用之號碼加以替換。其他變化系統資訊（遠離基地台，傳送層次等）可以用以替代GSM時鐘。鑰產生器指示可以不同地使用，例如在卡及終端上之微處理機可以假設完全負責加密，而不只是例如單元18及裝置22之專用單元。同樣地，所計算得之鑰之使用係基於SIM命令組之交談。本能上的熟習於本技藝者可採用不同基礎，不是單一傳送就是終端之整個活動週期。上述之實施例只是於目標應用中之較佳解決方案。

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

四、中文發明摘要(發明之名稱：傳送資訊於用戶識別模組及無線通訊行動終端間之方法；及相關用戶識別模組及行動終端)

一種用以傳送資訊於用戶識別模組及行動終端間之方法，該終端構成一無線通訊系統之一站台，於系統中至少部份被傳送於模組及終端間之資訊係藉由加密加以保護。用戶識別模組及行動終端包含加密機構，該機構使用一至少被部份專屬於該系統之週期變化資料所定義之鑰。

英文發明摘要(發明之名稱：)

A METHOD OF TRANSFERRING INFORMATION BETWEEN A SUBSCRIBER IDENTIFICATION MODULE AND A RADIOCOMMUNICATION MOBILE TERMINAL, AND A CORRESPONDING SUBSCRIBER IDENTIFICATION MODULE AND MOBILE TERMINAL

A method of transferring information between a subscriber identification model and a mobile terminal constituting a station of a radiocommunication system in which at least some of the information transferred between said module and said terminal is protected by encryption. The subscriber identification module and the mobile terminal include encryption means using a key defined at least in part by periodically-varying data specific to the system.

(請先閱讀背面之注意事項再填寫本頁各欄)

裝

訂

線

六、申請專利範圍

1. 一種傳送資訊於用戶識別模組及一行動終端之方法，該終端構成一無線通訊系統之一站台，其中至少部份被傳送於模組及終端間之資訊係藉由一用於該模組及終端中之一鑰之加密而加以保護，其中該鑰至少部份藉由該系統之週期變化資料所定義。

2. 如申請專利範圍第1項所述之資訊傳送方法，其中該週期變化資料係一專屬於該無線通訊系統之時鐘函數。

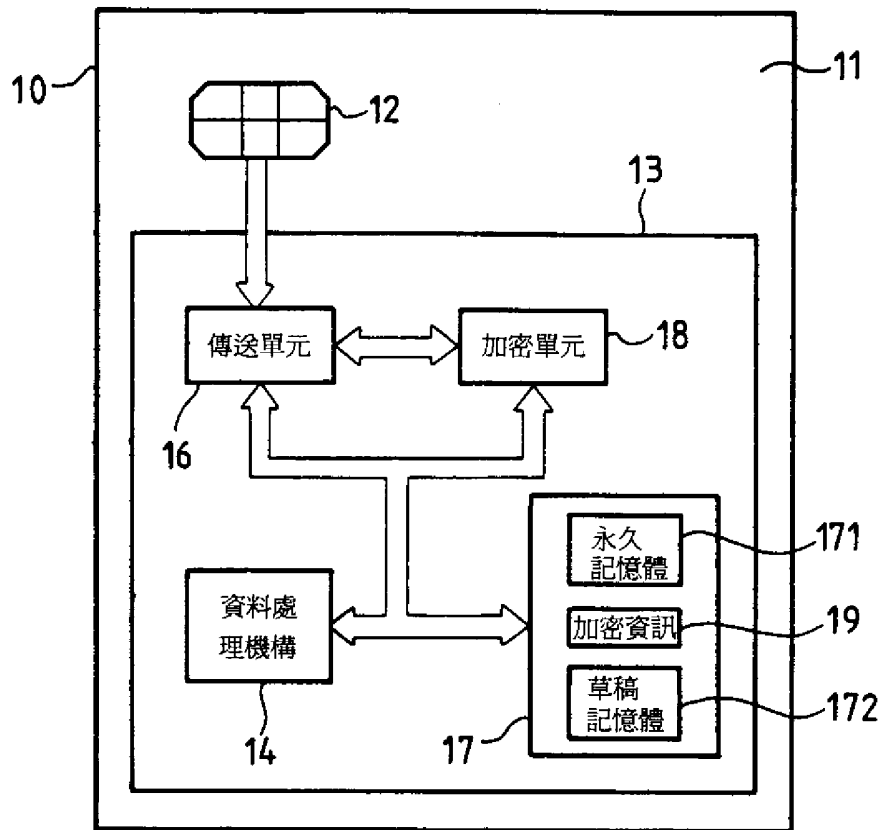
3. 如申請專利範圍第1項所述之資訊傳送方法，其中該鑰之至少另一部份係專屬於該行動台之資料所定義。

4. 如申請專利範圍第1項所述之資料傳送方法，其中該定義該鑰之資料係被組合於該模組及該終端中，於每一被加密所保護之資訊傳送之時。

(請先閱讀背面之注意事項再填寫本頁)

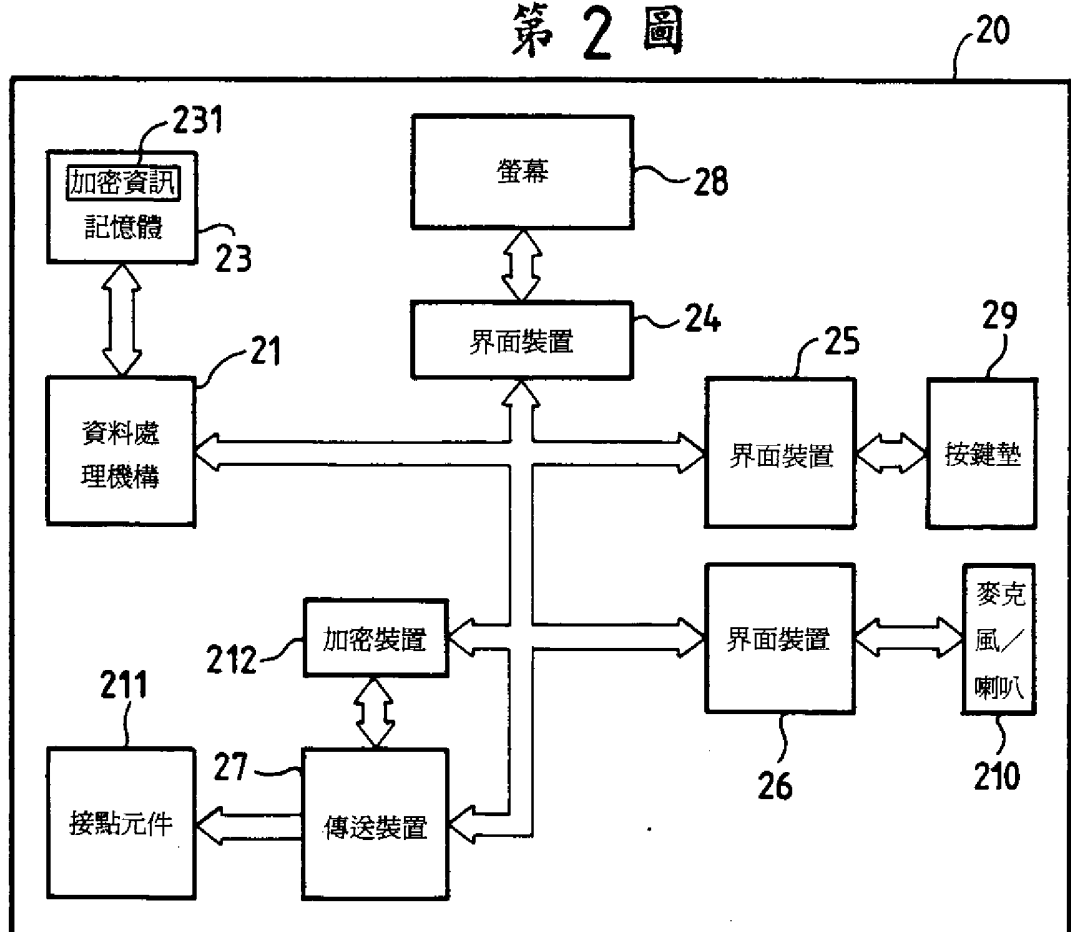
表

訂

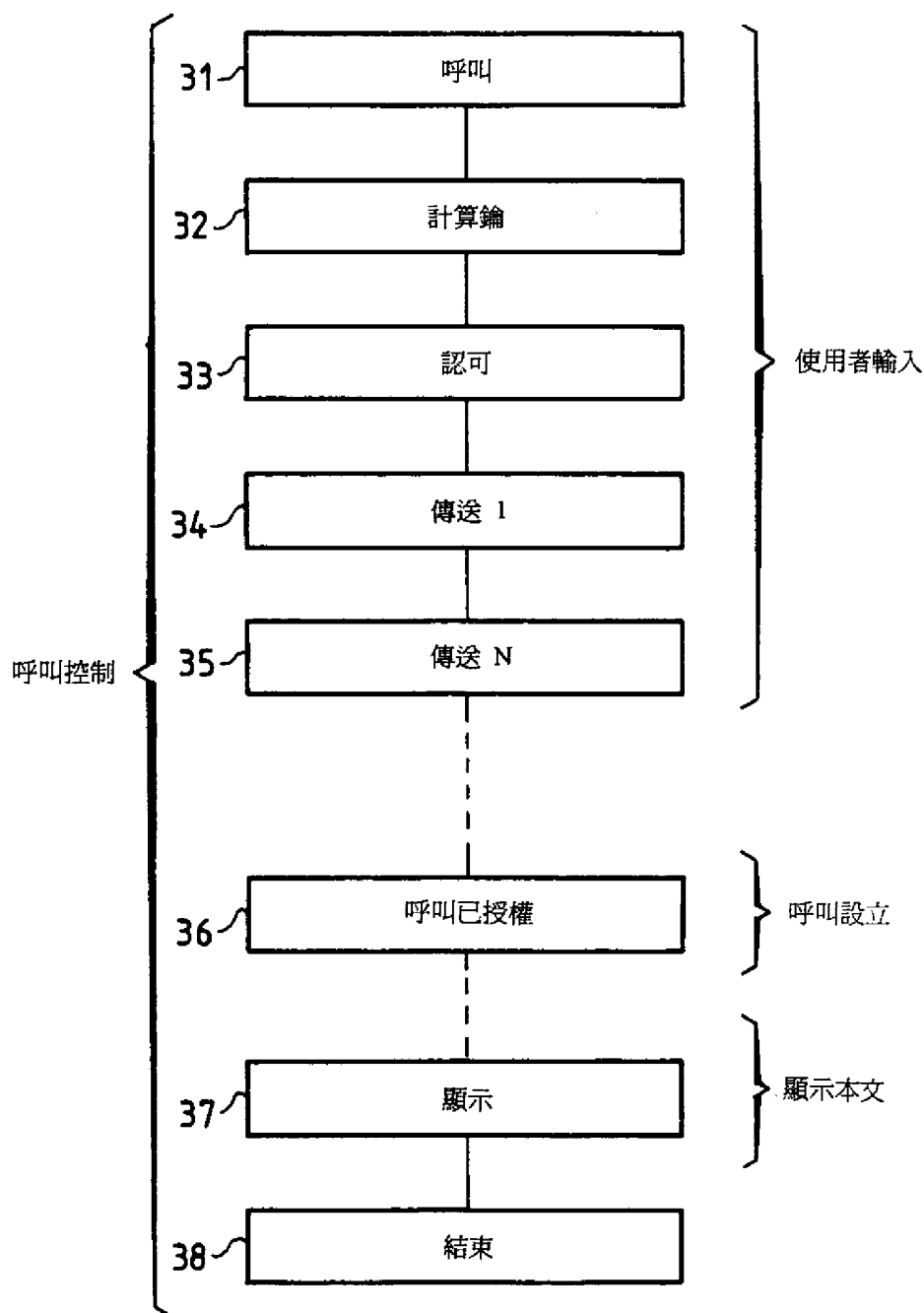


第 1 圖

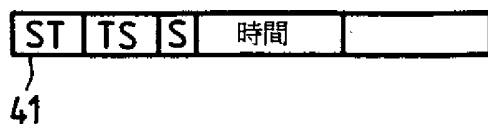
第 2 圖



第 3 圖



第 4 圖



第 5 圖

